Wireshark Packet Analysis Project Report

Project Title:

Real-Time Network Traffic Analysis Using Wireshark

Objective:

To capture and analyze real-time network traffic using Wireshark and identify potential security risks such as unencrypted data, suspicious DNS queries, brute-force attempts, and data exfiltration.

Tools Used:

- Wireshark
- Npcap
- Windows 11 / Kali Linux

Methodology:

1. Setup & Capture

Installed and launched Wireshark with admin privileges.

Selected the active network interface (Wi-Fi).

Captured live traffic for 5 minutes while browsing websites and running background apps.

2. Filtering & Analysis

Used Wireshark filters to inspect specific protocols and activities:

- http contains "password": Detect exposed credentials
- dns: Analyze domain name lookups
- tcp.port == 22: Monitor SSH traffic (brute-force attacks)
- ip.dst == [external IP]: Track outbound connections (data exfiltration)

3. Suspicious Activity Identified

- Found a login form transmitting credentials via HTTP (unencrypted).

- Repeated DNS queries to unknown domains (possible malware).

- Multiple failed SSH attempts from a single IP (brute-force).

- Large outbound data transfers (potential data exfiltration).

Security Recommendations:

- Enforce HTTPS on web apps

- Use SSH keys and fail2ban

- Implement DNS filtering

- Monitor outbound data and apply DLP solutions

Conclusion:

This project provided practical experience in analyzing network traffic and identifying threats. It highlights how attackers exploit vulnerabilities and how defenders can detect and respond to those threats.